Listing of Claims

1. (Currently Amended) Method for generating a second data stream from a first data stream which comprises a first header and a first payload data block with payload data, wherein the first header comprises a first supplier identification for a supplier of the first data stream and a first user identification for a receiver of the first data stream, the method comprising the following computer implemented steps:

extracting the first header from the first data stream;

generating a second header for the second data stream, wherein the second header comprises a second supplier identification for a supplier of the second data stream and a second user identification for a receiver of the second data stream;

entering at least a part of the first header into the second header, the part of the first header including information which allows conclusions as to the origin of the payload data, wherein the information comprises the first supplier identification for the supplier of the first data stream, and the first user identification for the receiver of the first data stream; and

generating a second payload data block having the same payload data as the payload data block of the first data stream, so as to obtain the second data stream;

wherein the payload data include audio data, video data, a combination of audio data and video data, or text data.

2. (canceled)

3. (Currently Amended) Method as claimed in claim 1, wherein the information allowing conclusions as to the origin of the first data stream further includes author information, such as ~~the~~ information on an author, or ~~the~~a ~~component~~composer, ~~the~~ an ISRC number, ~~the~~ an ISAN number or ~~the~~ an ISMN number of the payload data of the first data stream.

4. (canceled)

5. (Currently Amended) Method as claimed in claim 41, wherein the first user identification is device-specific, the method further comprising the step of ~~and the receiver~~ receiving ~~of~~ the first data stream ~~is~~ by a player or by a smart card indicated by the first user identification, ~~or a smart card~~.

6. (Original) Method as claimed in claim 1, wherein the part of the first header which is entered into the second header further comprises licence data relating to the manner in which a receiver of the first data stream may use the same, the licence data of the first header specifying the licence data of the second header.

7. (Currently Amended) Method as claimed in claim 6, wherein the licence data of the first header specify that the first data stream may be copied a certain number of times, that no copy may be taken of a copy, ~~however,~~ and wherein the step of generating the second header for the second data stream ~~including~~ includes the step of entering ~~of~~ second licence information into the second header of the second data stream, such that no more ~~copy~~ copies ~~may~~ are allowed to be taken of the second data stream.

8. (canceled)

9. (Original) Method as claimed in claim 1, which further comprises the following step:

issuing a digital signature for the second header, including the part of the first header, and attaching the digital signature to the second header.

10. (Original) Method as claimed in claim 9, wherein the issuing step further comprises the following substeps:

forming a hash sum over the second header, including the part of the first header, using a specified hash algorithm; and

encrypting the hash sum by means of an asymmetric encrypting method using a private key of the receiver of the first data stream.

11. (Original) Method as claimed in claim 1, wherein the payload data in the payload data block are at least partly encrypted and wherein encrypting information is contained in the first header, the step of generating the second header further comprising the following steps:

decrypting the first payload data block of the first data stream using the encrypting information in the first header;

encrypting the decrypted payload data and entering corresponding encrypting information into the second header,

the encrypting information of the first header also being entered into the second header.

12. (Currently Amended) Method as claimed in claim 11, wherein the encrypted payload data in the first payload data block are encrypted symmetrically using a key and wherein ~~the~~ the key is again encrypted asymmetrically using a private key, the decrypting step comprising the following steps:

decrypting the encrypted key by means of the public key of the supplier so as to obtain the key for a symmetric decryption;

encrypting a payload data key of the decrypted payload data using a private key of a receiver of the first data stream carrying out the method for generating a second data stream; and

entering the asymmetrically encrypted payload data key into the second header.

13. (Original) Method as claimed in claim 1, wherein in the step of entering, the entire first header is entered into the second header.

14. (Currently Amended) Method as claimed in claim 1, wherein the first header itself comprises at least a part of a header of a data stream which relates to the origin of the first data stream, such that the entering step results in a multiple~~y~~ recursive header structure.

15. (Currently Amended) Method for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, wherein at least a part of the first header which comprises information regarding the origin of the first data stream, wherein the information comprises a first supplier identification for a supplier of the first data stream, and the first user identification for a receiver of the first data stream, is contained in the second header, wherein the second header comprises a second supplier identification for a supplier of the second data stream and a second user identification for a receiver of the second data stream, the method comprising the following computer implemented steps:

extracting the part of the first header from the second header;

verifying the origin of the second data stream using the part of the first header which comprises information regarding the origin of the first data stream, wherein a positive result is obtained if the second supplier identification matches the first user identification, and wherein a negative result is obtained if the second supplier identification does not match the first user identification; ~~and~~

in case of a positive result of the verifying step, playing the second data stream; and

in case of a negative result of the verifying step, refusing to play the second data stream.

16. (Original) Method as claimed in claim 15, wherein the second header of the second data stream has a digital signature attached to it which fits the part of the first header, and wherein the verifying step comprises the following substep:

checking the authenticity of the second header using the digital signature.

17. (Original) Method as claimed in claim 16, wherein the digital signature is the result of an encryption of a hash sum of the second header, which

encryption has been carried out by means of a private key of the apparatus having generated the second data stream, the step of checking the authenticity comprising the following steps:

decrypting the digital signature by a public key of the apparatus which has generated the second data stream, so as to obtain the hash sum of the second header;

forming a hash sum of the present header;

comparing the hash sums;

in case of the hash sums matching, issuing a positive verification result.

18. (Original) Method as claimed in claim 17, wherein the part of the first header further comprises licence information regarding the manner in which the first data stream may be utilized, and wherein the second header comprises licence data derived from the licence data of the first header, the method further comprising the following substeps:

comparing the licence data of the second header and the first header so as to evaluate the authenticity of the licence data of the second header;

in case of questionable authenticity, blocking the playing of the second data stream.

19. (Currently Amended) Apparatus for generating a second data stream from a first data stream which comprises a first header and a first payload data block with payload data, wherein the first header comprises a first supplier identification for a supplier of the first data stream and a first user identification for a receiver of the first data stream, the apparatus comprising the following:

~~means~~ an extractor for extracting the first header from the first data stream;

~~means~~ a second header generator for generating a second header for the second data stream, wherein the second header comprises a second

supplier identification for a supplier of the second data stream and a second user identification for a receiver of the second data stream;

~~means~~ a processor for entering at least a part of the first header into the second header, the part of the first header including information which allow conclusions as to the origin of the payload data, wherein the information comprises a first supplier identification for a supplier of the first data stream, and the first user identification for a receiver of the first data stream; and

~~means~~ a second payload data block generator for generating a second payload data block which comprises the same payload data as the payload data block of the first data stream, so as to obtain the second data stream.

20. (Original) Apparatus as claimed in claim 19, which is designed as a personal computer.

21. (Currently Amended) Apparatus for playing a second data stream which comprises a second header and a second payload data block and has been generated due to a first data stream which comprises a first header and a first payload data block, at least a part of the first header, which comprises information regarding the origin of the first data stream, wherein the information comprises a first supplier identification for a supplier of the first data stream, and the first user identification for a receiver of the first data stream being contained in the second header, wherein the second header comprises a second supplier identification for a supplier of the second data stream and a second user identification for a receiver of the second data stream, the apparatus comprising the following:

~~means~~ an extractor for extracting the part of the first header from the second header;

~~means~~ a verifier for verifying the origin of the second data stream using the part of the first header which comprises information regarding the origin of the first data stream; and

~~means~~ a player for playing the second data stream, which responds to the means for verifying, so as to play the second data stream only if the means for verifying provide a positive result, and to refuse playing the second data stream in the case of a negative result.

22. (Original) Apparatus as claimed in claim 21, which is designed as a hifi system, as a car hifi system, as a portable multimedia player, as a computer or as a component of any of the above-mentioned devices.